United States General Accounting Office

GAO

Report to the Secretary of Veterans Affairs

September 1998

INFORMATION SYSTEMS

VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure

GAO/AIMD-98-175

GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-280049

September 23, 1998

The Honorable Togo D. West, Jr.
The Secretary of Veterans Affairs

Dear Mr. Secretary:

This report discusses weaknesses that we identified during our assessment of general computer controls that support key financial management and benefit delivery operations of the Department of Veterans Affairs (VA). General computer controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. They include security management, operating procedures, software security features, and physical protection designed to ensure that access to data is appropriately restricted, only authorized changes are made to computer programs, computer security duties are segregated, and backup and recovery plans are adequate to ensure the continuity of essential operations. Such controls are critical to VA's ability to safeguard assets, maintain the confidentiality of sensitive financial data and information on veteran medical records and benefit payments, and ensure the reliability of financial management information.

Our review of VA's general computer controls was performed in connection with the department's financial audit conducted under the Chief Financial Officers Act of 1990, as expanded by the Government Management Reform Act of 1994. The results of our evaluation of general computer controls were shared with VA's Office of Inspector General (OIG) for its use in auditing VA's consolidated financial statements for fiscal year 1997.

This report does not detail certain serious weaknesses in controls over access to VA computer resources. A separate report on those matters, with limited distribution due to its sensitive nature, is being issued today.

Results in Brief

General computer control weaknesses place critical VA operations, such as financial management, health care delivery, benefit payments, life insurance services, and home mortgage loan guarantees, and the assets associated with these operations, at risk of misuse and disruption. In addition, sensitive information contained in VA's systems, including financial transaction data and personal information on veteran medical records and benefit payments, is vulnerable to inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possibly occurring without detection. The general control weaknesses we identified could also diminish the reliability of the department's financial statements and other management information derived from VA's systems.

We found significant problems related to the department's control and oversight of access to its systems. VA did not adequately limit the access of authorized users or effectively manage user identifications (ID) and passwords. The department also had not established effective controls to prevent individuals, both internal and external, from gaining unauthorized access to VA systems. VA's access control weaknesses were further compounded by ineffective procedures for overseeing and monitoring systems for unusual or suspicious access activities.

In addition, the department was not providing adequate physical security for its computer facilities, assigning duties in such a way as to segregate incompatible functions, controlling changes to powerful operating system software, or updating and testing disaster recovery plans to prepare its computer operations to maintain or regain critical functions in emergency situations. Many of these access and other general computer control weaknesses are similar to weaknesses that have been previously identified by VA's OIG and consultant evaluations. Also, the OIG reported information system security controls as a material weakness in its report on VA's consolidated financial statements for fiscal year 1997.

A primary reason for VA's continuing general computer control problems is that the department does not have a comprehensive computer security planning and management program. An effective program would include guidance and procedures for assessing risks, establishing appropriate policies and related controls, raising awareness of prevailing risks and mitigating controls, and monitoring and evaluating the effectiveness of established controls. Such a program, if implemented completely across the department, would provide VA with a solid foundation for resolving existing computer security problems and managing its information security risks on an ongoing basis.

The VA facilities that we visited plan to address all of the specific computer control weaknesses identified. In fact, the director of the Austin Automation Center told us that his staff had corrected many of the general computer control weaknesses that we identified. The director of the Dallas Medical Center and the Veterans Benefits Administration Chief

Information Officer (CIO) also said that specific actions had been taken to correct the computer control weaknesses that we identified at the Dallas Medical Center and the Hines and Philadelphia benefits delivery centers. Furthermore, the Deputy Assistant Secretary for Information Resources Management told us that VA plans to develop a comprehensive security plan and management program.

Background

VA provides health care and other benefits to veterans in recognition of their service to our country. As of July 1, 1997, 26 percent of the nation's population—approximately 70 million persons who are veterans, veterans' dependents, or survivors of deceased veterans—was potentially eligible for VA benefits and services, such as health care delivery, benefit payments, life insurance protection, and home mortgage loan guarantees.

VA operates the largest health care delivery system in the United States and guarantees loans on about 20 percent of the homes in the country. In fiscal year 1997, VA spent more than $17 billion on medical care and processed more than 40 million benefit payments totaling more than $20 billion. The department also provided life insurance protection through more than 2.5 million policies that represented about $24 billion in coverage at the end of fiscal year 1997.

In providing these benefits and services, VA collects and maintains sensitive medical record and benefit payment information for millions of veterans and their dependents and survivors. VA also maintains medical information for both inpatient and outpatient care. For example, the department records admission, diagnosis, surgical procedure, and discharge information for each stay in a VA hospital, nursing home, or domiciliary. VA also stores information concerning health care provided to and compensation received by ex-prisoners of war. In addition, VA maintains information concerning each of the guaranteed or insured loans closed by VA since 1944, including about 3.5 million active loans.

VA relies on a vast array of computer systems and telecommunication networks to support its operations and store the sensitive information it collects in carrying out its mission. Three centralized data centers—located in Austin, Texas; Hines, Illinois; and Philadelphia, Pennsylvania—maintain the department's financial management systems; process compensation, pension, and other veteran benefit payments; and manage the veteran life insurance programs. In addition to the three centralized data centers, the Veterans Health Administration (VHA) operates 172 hospitals at locations across the country that operate local financial management and medical support systems on their own computer systems.

The Austin Automation Center maintains VA's departmentwide systems, including centralized accounting, payroll, vendor payment, debt collection, benefits delivery, and medical systems. In fiscal year 1997, VA's payroll was almost $11 billion and the centralized accounting system generated more than $7 billion in additional payments. The Austin Automation Center also provides, for a fee, information technology services to other government agencies. The center currently processes a workers compensation computer application for other federal agencies and plans to expand the computing services it provides to federal agencies.

The other two centralized data centers support VA's Veterans Benefits Administration (VBA) programs. The Hines Benefits Delivery Center processes information from VA systems that support the compensation, pension, and education applications for VBA's 58 regional offices. The Philadelphia Benefits Delivery Center is primarily responsible for supporting VA's life insurance program.

In addition, VHA hospitals operate local financial management and medical support systems on their own computer systems. The medical support systems manage information on veteran inpatient and outpatient care, as well as admission and discharge information, while the main medical financial system—the Integrated Funds Distribution, Control Point Activity, Accounting and Procurement (IFCAP) system—controls most of the $17 billion in funds that VA spent on medical care in fiscal year 1997. The IFCAP system also transmits financial and inventory information daily to the Financial Management System in Austin.

The three VA data centers, as well as the 172 VHA hospitals, 58 VBA regional offices, and the VA headquarters office, are all interconnected through a wide area network. All together, VA's network serves more than 40,000 on-line users.

Objective, Scope, and Methodology

Our objective was to evaluate and test the effectiveness of general computer controls over the financial systems maintained and operated by VA at its Austin, Hines, and Philadelphia data centers as well as selected VA medical centers. General computer controls, however, also affect the security and reliability of nonfinancial information, such as veteran medical, loan, and insurance data, maintained at these processing centers.

At the Austin Automation Center and VA medical centers in Dallas and Albuquerque, we evaluated controls intended to

- protect data and application programs from unauthorized access;
- prevent the introduction of unauthorized changes to application and system software;
- provide segregation of duties involving application programming, system programming, computer operations, security, and quality assurance;
- ensure recovery of computer processing operations in case of a disaster or other unexpected interruption; and
- ensure that an adequate computer security planning and management program is in place.

The scope of our work at the Hines and Philadelphia benefits delivery centers was limited to (1) evaluating the appropriateness of access granted to selected individuals and computer resources, (2) assessing efforts to monitor access activities, and (3) examining the computer security administration structure. We restricted our evaluation at the Hines and Philadelphia benefits delivery centers because VA's OIG was planning to perform a review of other general computer controls at these sites during fiscal year 1997.

To evaluate computer controls, we identified and reviewed VA's information system general control policies and procedures. Through this review and discussions with VA staff, including programming, operations, and security personnel, we determined how the general computer controls were intended to work and the extent to which center personnel considered them to be in place. We also reviewed the installation and implementation of VA's operating system and security software.

Further, we tested and observed the operation of general computer controls over VA's information systems to determine whether they were in place, adequately designed, and operating effectively. To assist in our evaluation and testing of general computer controls, we contracted with Ernst & Young LLP. We determined the scope of our contractor's audit work, monitored its progress, and reviewed the related work papers to ensure that the resulting findings were adequately supported.

We performed our work at the VA data centers in Austin, Hines, and Philadelphia; the VA medical centers in Dallas and Albuquerque; and VA headquarters in Washington, D.C., from October 1997 through January 1998. Our work was performed in accordance with generally accepted government auditing standards.

VA provided us with written comments on a draft of this report, which are discussed in the "Agency Comments" section and reprinted in appendix I.

Access to Data and Programs Is Not Adequately Controlled

A basic management objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modification, disclosure, or deletion. Our review of VA's general computer controls found that the department was not adequately protecting financial and sensitive veteran medical and benefit information. Specifically, VA did not adequately limit the access granted to authorized VA users, properly manage user IDs and passwords, or routinely monitor access activity. As a result, VA's computer systems, programs, and data are at risk of inadvertent or deliberate misuse, fraudulent use, and unauthorized alteration or destruction occurring without detection.

We also found that VA had not adequately protected its systems from unauthorized access from remote locations or through the VA network. The risks created by these security issues are serious because in VA's interconnected environment, the failure to control access to any system connected to the network also exposes other systems and applications on the network. Due to the sensitive nature of the remote access and network control weaknesses we identified, these issues are described in a separate report with limited distribution issued to you today.

Access Authority Is Not Appropriately Limited for Authorized VA Users

A key weakness in VA's internal controls was that the department was not adequately limiting the access of VA employees. Organizations can protect information from unauthorized changes or disclosures by granting employees authority to read or modify only those programs and data that are necessary to perform their duties.

VA, however, allowed thousands of users to have broad authority to access financial and sensitive veteran medical and benefit information. At Austin, for example, the security software was implemented in a manner that provided all of the more than 13,000 users with the ability to access and change sensitive data files, read system audit information, and execute powerful system utilities. Such broad access authority increased the risk that users could circumvent the security software, and presented users with an opportunity to alter or delete any computer data or program. The director of the Austin Automation Center told us that his staff had restricted access to the sensitive data files, system audit information, and powerful system utilities that we identified.

In addition, we found several other examples where VA did not adequately restrict the access of legitimate users, including the following.

- At both the Hines and Philadelphia centers, we found that system programmers had access to both system software and financial data. This access could allow the programmers to make changes to financial information without being detected.
- At the Hines center, we also identified 18 users in computer operations who could update sensitive computer libraries. Update access to these libraries could result in the security software being circumvented with the use of certain programs to alter or delete sensitive data.
- At the Dallas center, we determined that 12 computer support personnel had access to all financial and payroll programs and data. Although these support staff need access to certain programs, providing complete access weakens the organization's ability to ensure that only authorized changes are allowed.
- At the Austin center, we found more than 100 users who had an access privilege that provided the ability to bypass security controls and enabled them to use any command or transaction. Access to this privilege should be limited to use in emergencies or for special purposes because it creates a potential security exposure.

The director of the Austin Automation Center told us that the privilege that provided users the opportunity to bypass security controls had been removed from all individual user IDS. The VBA CIO also said that a task force established to address control weaknesses had evaluated the inappropriate access that we identified at the Hines and Philadelphia benefits delivery centers and made recommendations for corrective measures.

We also found that VA was not promptly removing access authority for terminated or transferred employees or deleting unused or unneeded IDS.

- At the Dallas and Albuquerque centers, we found that IDS belonging to terminated and transferred employees were not being disabled. We identified over 90 active IDs belonging to terminated or transferred employees at Dallas and 50 at Albuquerque. If user IDs are not promptly disabled when employees are terminated, former employees are allowed the opportunity to sabotage or otherwise impair VA operations.

- At the Dallas center, we identified more than 800 IDs that had not been used for at least 90 days. We also identified inactive IDs at the Austin, Hines, and Albuquerque centers. For instance, at the Hines center, we found IDs that had been inactive for as long as 7 years. Allowing this situation to persist poses unnecessary risk that unneeded IDs will be compromised to gain unauthorized access to VA computer systems.

In January 1998, the director of the Dallas Medical Center said that a program had been implemented to disable all user IDs for terminated employees and those IDs not used in the last 90 days. In addition, the director of the Austin Automation Center and the VBA CIO told us that IDs would be automatically suspended 30 days after the password expired at the Austin, Hines, and Philadelphia centers.

One reason that VA's user access problems existed was because user access authority was not being reviewed periodically. Such periodic reviews would have allowed VA to identify and correct inappropriate access.

The directors of the Austin Automation Center and the Dallas Medical Center told us that they planned to periodically review system access. The VBA CIO also said that the Hines and Philadelphia benefits delivery centers will begin routinely reviewing user IDs and deleting individuals accordingly.

User ID and Password Management Controls Are Not Effective

In addition to overseeing user access authority, it is also important to actively manage user IDs and passwords to ensure that users can be identified and authenticated. To accomplish this objective, organizations should establish controls to maintain individual accountability and protect the confidentiality of passwords. These controls should include requirements to ensure that IDs uniquely identify users; passwords are changed periodically, contain a specified number of characters, and are not common words; default IDs and passwords are changed to prevent their use; and the number of invalid password attempts is limited. Organizations should also evaluate the effectiveness of these controls periodically to ensure that they are operating effectively. User IDs and passwords at the sites we visited were not being effectively managed to ensure individual accountability and reduce the risk of unauthorized access.

VA had issued an updated security policy in January 1997 that addressed local area network user ID and password management. Specifically, this policy required users to have separate IDs; passwords to be changed periodically, be at least six characters in length, and be formed with other than common words; and IDs to be suspended after three invalid password attempts. Despite these requirements, we identified a pattern of network control weaknesses because VA did not periodically review local area network user IDs and passwords for compliance with this policy.

- At the Albuquerque center, we identified 119 network IDs that were allowed to circumvent password change controls, 15 IDs that did not have any passwords, and eight IDs that had passwords with less than six characters.
- At the Philadelphia center, we found that approximately half of the network user IDs, including the standard network administrator ID, were vulnerable to abuse because passwords were common words that could be easily guessed or found in a dictionary.
- At the Austin and Dallas centers, we found that network passwords were set to never expire. Not requiring passwords to be changed increases the risk that they will be uncovered, which could lead to unauthorized access.

In February 1998, the VBA CIO told us that the Hines and Philadelphia benefits delivery centers plan to require that passwords not be common words. Additionally, the directors of both the Austin Automation Center and the Dallas Medical Center said that although their staffs did not control wide area network password management controls, they were working with VA technical staff to improve network password management by requiring passwords to be changed periodically.

In addition, VA's user ID and password management policy only applied to local area networks. VA did not have departmentwide policies governing user IDs and passwords for other computer platforms, such as mainframe computers or the wide area network. Although some organizations within VA had procedures in these areas, we identified a number of user ID and password management problems.

- At the Philadelphia center, we found that the security software was implemented in a manner that did not disable the master security administration ID after a specified number of invalid password attempts.

Allowing unlimited password attempts to this ID, which has the highest level security authority, increases the risk of unauthorized access to or disclosure of sensitive information.

- At the Austin center, we determined that more than 100 mainframe IDs that did not require passwords, many of which had broad access authority, were not properly defined to prevent individuals from using them. Although system IDs without passwords are required to perform certain operational tasks, these IDs should not be available to individual users because IDs that do not require password validation are more susceptible to misuse. Twenty of these IDs were especially vulnerable to abuse because the account identifiers were common words, software product names, or derivations of words or products that could be easily guessed.
- At the Dallas and Albuquerque centers, we discovered that an ID established by a vendor to handle various support functions had remained active even though the vendor had recommended that this ID be suspended when not in use.

The director of the Austin Automation Center told us that his staff had deleted nearly 50 of the mainframe IDs that did not require passwords and reduced the access authority for many of the remaining IDs that did not require passwords. In addition, the chief of the Information Resources Management Service at the Dallas Medical Center agreed to take steps to address the system maintenance ID problem we identified.

We also found numerous instances where user IDs and passwords were being shared by staff. For example, as many as 16 users at the Albuquerque Medical Center and an undetermined number at the Dallas Medical Center were sharing IDs with privileges to all financial data and system software. At Austin, more than 10 IDs with high-level security access were being shared by several staff members. The use of shared IDs and passwords increases the risk of a password being compromised and undermines the effectiveness of monitoring because individual accountability is lost.

The director of the Austin Automation Center told us that shared IDs had been eliminated and replaced with individually assigned user IDs. In addition, the chief of the Information Resources Management Service at the Dallas Medical Center agreed to take steps to address the shared ID problem we identified.

Access Activities Are Not Being Monitored

The risks created by these access control problems were also heightened significantly because the sites we visited were not adequately monitoring system and user access activity. Routinely monitoring the access activities of employees, especially those who have the ability to alter sensitive programs and data, can help identify significant problems and deter employees from inappropriate and unauthorized activities. Without these controls, VA had little assurance that unauthorized attempts to access sensitive information would be detected.

Because of the volume of security information that must be reviewed, the most effective monitoring efforts are those that target specific actions. These monitoring efforts should include provisions to review

- unsuccessful attempts to gain entry to a system or access sensitive information,
- deviations from access trends,
- successful attempts to access sensitive data and resources,
- highly-sensitive privileged access, and
- access modifications made by security personnel.

For VA, such an approach could be accomplished using a combination of the audit trail capabilities of its security software and developing computerized reports. This approach would require each facility to compile a list of sensitive system files, programs, and software so that access to these resources could be targeted. Access reports could then be developed for security staff to identify unusual or suspicious activities. For instance, the reports could provide information on browsing trends or summarizations based on selected criteria that would target specific activities, such as repeated attempts to access certain pay tables or sensitive medical and benefit information.

Despite the thousands of employees who had legitimate access to VA computer systems containing financial and operational data, VA did not have any departmentwide guidance for monitoring successful and unsuccessful attempts to access system files containing key financial information or sensitive veteran data. As a result, VA's monitoring efforts were not effective for detecting unauthorized access to or modification of sensitive information.

The security staffs at the Philadelphia, Hines, Dallas, and Albuquerque centers were not actively monitoring access activities. At the Philadelphia center, available violation reports were not being reviewed, while at the Hines center, it was unclear who had specific responsibility for monitoring access. As a result, no monitoring was being performed at either the Hines or Philadelphia centers. In addition, neither the Dallas nor Albuquerque centers had programs to actively monitor access activities.

Also, violation reports at the Austin Automation Center did not target most types of unusual or suspicious system activity, such as repeated attempts to access sensitive files or libraries or attempts to access certain accounts or pay tables. In addition, the Austin Automation Center had not developed any browsing trends or instituted a program to monitor staff access, particularly access by staff who had significant access authority to critical files, programs, and software.

The director of the Austin Automation Center told us that he plans to establish a new security staff that will be responsible for establishing a targeted monitoring program to identify access violations, ensure that the most critical resources are properly audited, and periodically review highly privileged users, such as system programmers and security administrators. Also, the director of the Dallas Medical Center told us that his staff plan to periodically review user access. In addition, the chief of the Information Resources Management Service told us during follow-up discussions that the Dallas Medical Center will establish a targeted monitoring program to review access activities.

Furthermore, none of the five sites we visited were monitoring network access activity. Although logging events on the network is the primary means of identifying unauthorized users or unauthorized usage of the system by authorized users, two of the sites we reviewed were not logging network security events. Unauthorized network access activity would also go undetected at the sites that were logging network activity because the network security logs were not reviewed.

The director of the Austin Automation Center told us that his staff planned to begin a proactive security monitoring program that would include identifying and investigating unauthorized attempts to gain access to Austin Automation Center computer systems and improper access to sensitive information on these systems. The director of the Dallas Medical Center also told us that his staff planned to implement an appropriate network monitoring program.

Other General Controls Are Not Sufficient

In addition to these general access controls, there are other important controls that organizations should have in place to ensure the integrity and reliability of data. These general computer controls include policies, procedures, and control techniques to physically protect computer resources and restrict access to sensitive information, provide appropriate segregation of duties among computer personnel, prevent unauthorized changes to operating system software, and ensure the continuation of computer processing operations in case of an unexpected interruption. Although we did not review these general controls at the Hines and Philadelphia centers, we found weaknesses in these areas at the Albuquerque, Dallas, and Austin centers.

Physical Security Controls Are Not Effective

Important general controls for protecting access to data are the physical security control measures, such as locks, guards, fences, and surveillance equipment that an organization has in place. At VA, such controls are critical to safeguarding critical financial and sensitive veteran information and computer operations from internal and external threats. We found weaknesses in physical security at each of the three facilities where these controls were reviewed.

None of the three facilities that we visited adequately controlled access to the computer room. Excessive access to the computer rooms at these facilities was allowed because none of the sites had established policies and procedures for periodically reviewing access to the computer room to determine if it was still required. In addition, the Albuquerque Medical Center was not documenting access to the computer room by individuals who required escort, such as visitors, contractors, and maintenance staff.

At the Austin Automation Center, for instance, we found that more than 500 people had access to the computer room, including more than 170 contractors. The director of the Austin Automation Center told us that since our review, access to the computer room had been reduced to 250 individuals and that new policies and procedures would be established to further scrutinize the number of staff who had access to the computer room.

In addition, both the Dallas and Albuquerque medical centers gave personnel from the information resource management group unnecessary access to the computer room. At the Albuquerque Medical Center, 18 employees from the information resource management group had access to the computer room, while at the Dallas Medical Center, all information resource management staff were allowed access. At both medical centers, this access included personal computer maintenance staff and certain administrative employees who should not require access to the computer room. While it is appropriate for information resource management staff to have access to the computer room, care should be taken to limit access to only those employees who have a reasonable need.

Our review also identified other physical security control weaknesses. For example, windows in the Dallas Medical Center computer room were not alarmed to detect potential intruders and sensitive cabling in this computer room was not protected to prevent disruptions to computer operations. In addition, chemicals that posed a potential hazard to employees and computer operations were stored inside the computer room in Austin. Furthermore, a telecommunication panel in the Austin Automation Center computer room was also not protected, increasing the risk that network communications could be inadvertently disrupted.

The director of the Austin Automation Center told us that his staff had removed chemicals from the computer room and protected the telecommunications panel. In addition, the director of the Dallas Medical Center told us that his staff plan to address the physical security problems when the computer room is moved to a new facility.

Computer Duties Are Not Properly Segregated

Another fundamental technique for safeguarding programs and data is to segregate the duties and responsibilities of computer personnel to reduce the risk that errors or fraud will occur and go undetected. Duties that should be separated include application and system programming, quality assurance, computer operations, and data security.

At the Austin Automation Center, we found three system programmers who had been assigned to assist in the security administration function. Under normal circumstances, backup security staff should report to the security administrator and have no programming duties. Because these individuals had both system and security administrator privileges, they had the ability to eliminate any evidence of their activity in the system.

At the time of our review, Austin's security software administrator also reported to the application programming division director. The security software administrator, therefore, had application programming responsibility, which is not compatible with the duties associated with system security.

The director of the Austin Automation Center told us that actions had been taken to address the reported weaknesses. These actions included removing the master security administration user ID and password from system programmers and establishing a new security group to consolidate security software administration. During a follow-up discussion, the director also said that an emergency ID had been established to provide system programmers with additional access when required. This approach should not only improve access controls but also provide a means to determine if system programmer access authorities need to be expanded.

We also found instances where access controls did not enforce segregation of duties principles. For example, we found nine users in the information resource management group at the Albuquerque Medical Center who had both unrestricted user access to all financial data and electronic signature key authority. These privileges would allow the users to prepare invoices and then approve them for payment without creating an audit trail.

Changes to System Software Are Not Adequately Controlled

A standard computer control practice is to ensure that only authorized and fully tested operating system software is placed in operation. To ensure that changes to the operating system software are needed, work as intended, and do not result in the loss of data and program integrity, these changes should be documented, authorized, tested, independently reviewed, and implemented by a third party. We found weaknesses in operating system software change control at the Austin Automation Center.

Although the Austin Automation Center security policy required operating system software changes to be approved and reviewed, the center had not established detailed written procedures or formal guidance for modifying operating system software. There were no formal guidelines for approving and testing operating system software changes. In addition, there were no detailed procedures for implementing these changes.

During fiscal year 1997, the Austin Automation Center made more than 100 system software changes. However, none of these changes included evidence of testing, independent review, or acceptance. In addition, the Austin Automation Center did not provide any evidence of review by technical management. Furthermore, operating system software changes were not implemented by an independent control group.

The director of the Austin Automation Center told us that his staff planned to document and implement operating system software change control procedures that require independent supervisory review and approval. In addition, the director said that management approval will be required for each phase of the software change process.

Disaster Recovery Planning Is Not Complete

An organization must take steps to ensure that it is adequately prepared to cope with a loss of operational capability due to earthquakes, fires, accidents, sabotage, or any other disruption. An essential element in preparing for such catastrophes is an up-to-date, detailed, and fully tested disaster recovery plan. Such a plan is critical for helping to ensure that information systems can promptly restore operations and data, such as payroll processing and related records, in the event of disaster.

The disaster recovery plan for the Austin Automation Center consisted of 17 individual plans covering various segments of the organization. However, there was no overall document that integrated the 17 individual plans and set forth the roles and responsibilities of each disaster recovery team, defined the reporting lines between each team, and identified who had overall responsibility for the coordination of all 17 teams.

We also found that although the Austin Automation Center had tested its disaster recovery plan, it had only performed limited testing of network communications. This testing included the Austin Finance Center, but did not involve other types of users, such as VHA medical centers or VBA regional offices. In addition, the Austin Automation Center had not conducted unannounced tests of its disaster recovery plan, a scenario more likely to be encountered in the event of an actual disaster. Finally, a copy of the disaster recovery plan was not maintained at the off-site storage facility. In the event of a disaster, it is a good practice to keep at least one current copy of the disaster recovery plan at this location to ensure that it is not destroyed by the same events that made the primary data processing facility unavailable.

The director of the Austin Automation Center told us that he was in the process of correcting each of the deficiencies we identified. Actions he identified included (1) expanding network communication testing to include an outpatient clinic and a regional office, (2) conducting unannounced tests of the disaster recovery plan, (3) incorporating the 17 individual recovery plans into an executive plan, and (4) maintaining a copy of the disaster recovery plan at the off-site storage facility.

We found deficiencies in the disaster recovery planning at the Dallas and Albuquerque medical centers as well. At both locations (1) tests of the disaster recovery plans had not been conducted, (2) copies of the plans were not maintained off-site, (3) backup files for programs, data, and software were not stored off-site, and (4) periodic reviews of the disaster recovery plans were not required to keep them current.

The director of the Dallas Medical Center told us that he intends to review the disaster recovery plan semiannually, develop procedures to test the plan, and identify an off-site storage facility for both the disaster recovery plan and backup files.

Computer Security Problems Are Not New at VA

The general computer control weaknesses that we identified are similar to computer security problems that have been previously identified in evaluations conducted by VA's OIG and in contractor studies.

For example, in a July 1996 report evaluating computer security at the Austin Automation Center, the OIG stated that the center's security function was fragmented, user IDs for terminated employees were still active and being used, monitoring of access activities was not being performed routinely, over 600 individuals were authorized access to the computer room, and telecommunication connections were not fully tested during disaster recovery plan testing.

Similar findings were also identified by contractors hired by the Austin Automation Center to review the effectiveness of certain aspects of its general computer controls. Specifically, Austin brought in outside contractors to evaluate security software implementation in November 1995 and network security in April 1997. The security software review determined that key operating system libraries, security software files, and sensitive programs were not adequately restricted, that more than 90 IDs did not require passwords, and that access activity was not consistently monitored. In addition, the network security review found that the center had not established a comprehensive system security policy that included network security.

The OIG also reported comparable access control and security management problems at the Hines Benefits Delivery Center in May 1997. For example, the OIG determined that access to sensitive data and programs had not been appropriately restricted and that system access activity was not reviewed regularly to identify unauthorized access attempts. The OIG also found that security efforts at the Hines Benefits

Delivery Center needed to be more focused to meet the demands of the center.

In addition, the OIG identified general computer control weaknesses at seven VA medical centers as part of a review of the IFCAP system conducted from January 1994 to November 1995. Problems identified at a majority of these medical centers were reported in March 1997. These issues included problems with restricting access to the production environment, monitoring access activity, managing user IDs and passwords, testing disaster recovery plans, and reviewing user access privileges periodically.

Furthermore, the OIG included information system security controls as a material weakness in its report on VA's consolidated financial statements for fiscal year 1997. The OIG concluded that VA assets and financial data were vulnerable to error or fraud because of significant weaknesses in computer controls. Although the Federal Managers' Financial Integrity Act (FMFIA) of 1982 requires agencies to establish controls that reasonably ensure that assets are safeguarded against waste, loss, or unauthorized use, these information system integrity weaknesses were not included in the department's FMFIA report as a material internal control weakness in fiscal year 1997.

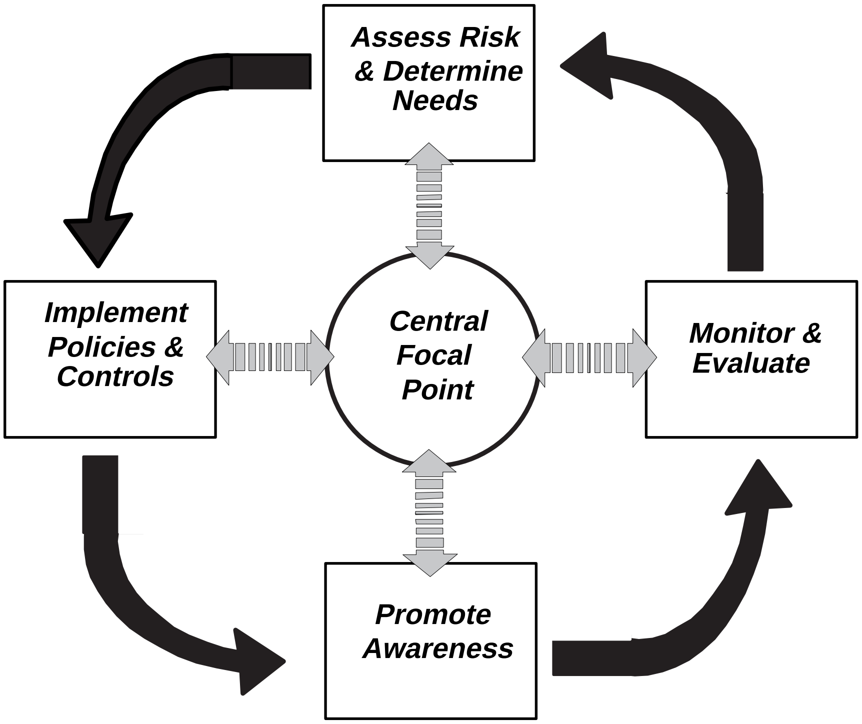
Computer Security Planning and Management Program Is Not Adequate

A key reason for VA's general computer control problems was that the department did not have a comprehensive computer security planning and management program in place to ensure that effective controls were established and maintained and that computer security received adequate attention.

To assist agencies in developing more comprehensive and effective information security programs, we studied the security management practices of eight nonfederal organizations with reputations as having superior information security programs. We found that these organizations successfully managed their information security risks through an ongoing cycle of risk management activities.[1] As shown in figure 1, each of these activities is linked in a cycle to help ensure that business risks are continually monitored, policies and procedures are regularly updated, and controls are in effect.

[1] For more information on the risk management cycle, see Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).

Figure 1: Risk Management Cycle



The risk management cycle begins with an assessment of risks and a determination of needs. This assessment includes selecting cost-effective policies and related controls. Once policies and controls are selected, they must be implemented. Next, the policies and controls, as well as the risks that prompted their adoption, must be communicated to those responsible for complying with them. Finally, and perhaps most important, there must be procedures for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can take appropriate corrective action. In addition, our study found that a strong central security management focal point can help ensure that the major elements of the risk management cycle are carried out and can serve as a communications link among organizational units.

In contrast, VA had not instituted a framework for assessing and managing risks or monitoring the effectiveness of general computer controls. Specifically, VA's computer security efforts lacked

- clearly delineated security roles and responsibilities;
- regular, periodic assessments of risk;
- security policies and procedures that addressed all aspects of VA's interconnected environment;
- an ongoing security monitoring program to identify and investigate unauthorized, unusual, or suspicious access activity; and
- a process to measure, test, and report on the continued effectiveness of computer system, network, and process controls.

The first key problem at the locations we reviewed was that security roles and responsibilities were not clearly assigned and security management was not given adequate attention. For example, the computer security administration function at the Austin Automation Center was fragmented between computer security administration staff and other computer security components. Specifically, computer security administration staff reported to the application programming division while other computer security staff reported to a staff function within the center's management directorate. Furthermore, the computer security administration staff was responsible for application programming in addition to supporting security administration.

The director of the Austin Automation Center told us that a new security group would be formed to consolidate staff performing the security software administration and physical security functions into one group. As part of this effort, roles and responsibilities for security administration were to be explicitly assigned.

The roles and responsibilities for managing computer security at the other facilities we reviewed were also weak. For instance, computer security administration at the Philadelphia Benefits Delivery Center was limited to adding and removing users from the system, while at the Hines Benefits Delivery Center the responsibility for day-to-day security monitoring and reviewing the overall effectiveness of the security program was unclear. And at both the Dallas and Albuquerque medical centers, security administration was assigned only as a collateral responsibility. The security administrators at these medical centers reported spending less than a fifth of their time on security-related matters, which was not sufficient to actively manage and monitor access to critical medical and financial systems.

A second key aspect of computer security planning and management is periodically assessing risk. Regular risk assessments assist management in making decisions on necessary controls by helping to ensure that security resources are effectively distributed to minimize potential loss. These assessments also increase the awareness of risks and, thus, generate support for adopted policies and controls, which helps ensure that the policies and controls operate as intended.

VA's policy requires that risk assessments be performed every 3 years or when significant changes are made to a facility or its computer systems. However, none of the three facilities where risk assessments were reviewed—Albuquerque, Dallas, and Austin—had completed risk assessments on a periodic basis or updated these assessments when significant changes occurred. For example, there was no indication that a risk assessment had ever been performed at the Albuquerque Medical Center. The Dallas Medical Center risk assessment had not been updated since 1994, even though its processing environment had changed significantly since then. The Dallas Medical Center has upgraded its computer hardware and added network capabilities since 1994. Furthermore, the Austin Automation Center did not conduct a risk assessment from 1991 through 1996, even though the center implemented a new financial management computer system during this period. The director of the Austin Automation Center told us that his staff planned to begin assessing risk on a regular basis.

A third key element of effective security planning and management is having established policies and procedures governing a complete computer security program. Such policies and procedures should integrate all security aspects of an organization's interconnected environment, including local area network, wide area network, and mainframe security. The integration of network and mainframe security is particularly important as computer systems become more and more interconnected.

VA's CIO, through the Deputy Assistant Secretary for Information Resources Management (DAS/IRM), is responsible for developing departmentwide security policies and periodically reviewing organizational compliance with the security policies. On January 30, 1997, DAS/IRM issued an updated security policy. However, this policy is still evolving and does not yet adequately establish a framework for developing and implementing effective security techniques or monitoring the effectiveness of these techniques within VA's interconnected environment. For example, the updated security policy addressed local area networks but did not provide guidance for other computer platforms, such as mainframe computer security.

A fourth key area of an overall computer security management program is an ongoing security monitoring program that helps to ensure that facilities are monitoring both successful and unsuccessful access activities. As noted above, VA did not have overall guidance on monitoring and evaluating access activities at VA processing facilities. Security administration staff at the VA facilities we visited were not actively monitoring successful or unsuccessful attempts to access sensitive computer system files. In addition, although VA has procedures for reporting computer security incidents, these procedures will not be effective until each facility establishes a mechanism for identifying computer security incidents.

A fifth key element of effective security planning and management is a process for periodically monitoring, measuring, testing, and reporting on the continued effectiveness of computer system, network, and process controls. This type of security oversight is an essential aspect of an overall security planning and management framework because it helps the organization take responsibility for its own security program and can help identify and correct problems before they become major concerns.

Although VA had taken some measures to evaluate controls periodically, the department had not established a coordinated program that provided for ongoing local oversight and periodic external evaluations. In addition, VA had not provided technical standards for implementing security software, maintaining operating system integrity, or controlling sensitive utilities. Such standards would not only help ensure that appropriate computer controls were established consistently throughout the department, but also facilitate periodic reviews of these controls.

The Austin Automation Center was the only facility we visited that had attempted to evaluate the effectiveness of its computer controls. For the last 3 years, the Austin Automation Center has brought in either OIG or contractor personnel to evaluate certain aspects of its computer security, including mainframe security software implementation, the network security environment, and physical access controls. In addition, the director of the Austin Automation Center told us that the center's client server environment and security controls would be reviewed during calendar year 1998. However, the Austin Automation Center had not established an ongoing security oversight program to ensure that controls continued to work as intended.

In addition, both the DAS/IRM security group and the VHA Medical Information Security Service (MISS) had performed security reviews, but these reviews focused on compliance rather than on the effectiveness of controls. The DAS/IRM security group evaluated disaster recovery on a departmentwide basis in fiscal year 1997; MISS reviews computer security at VHA processing facilities on a 3-year rotational basis. Despite these efforts, we found control weaknesses due to noncompliance with VA policies and procedures. Furthermore, until VA establishes a program to periodically evaluate the effectiveness of controls, it will not be able to ensure that its computer systems and data are adequately protected from unauthorized access.

In April 1998, DAS/IRM officials told us that VA is in the process of developing a comprehensive security plan and management program that will incorporate a risk management cycle and include requirements for monitoring access activity, reporting security incidents, and reviewing compliance with policies and procedures. The director of VHA MISS also told us in April 1998 that the VHA information security program office is addressing all of the security issues identified. As part of this effort, MISS plans to change its on-site security review procedures and VHA plans to expand current security policies and guidance.

Conclusions

VA's access control problems, as well as other general computer control weaknesses, are placing sensitive veteran medical and benefit information at risk of disclosure, critical financial and benefit delivery operations at risk of disruption, and assets at risk of loss. The general computer control weaknesses we identified could also adversely affect other agencies that depend on the Austin Automation Center for computer processing support.

Especially disturbing is the fact that many similar weaknesses had been reported in previous years, indicating that VA's past actions have not been effective on a departmentwide basis. Implementing more effective and lasting controls that protect sensitive veteran information and establish an effective general computer control environment requires that the department establish a comprehensive computer security planning and management program. This program should provide for periodically assessing risks, implementing effective controls for restricting access based on job requirements and proactively reviewing access activities, clearly defining security roles and responsibilities, and, perhaps most important, monitoring and evaluating the effectiveness of controls and policies to ensure that they remain effective.

Recommendations

We recommend that you direct the VA CIO to work in conjunction with the VBA and VHA CIOs and the facility directors as appropriate to

- limit access authority to only those computer programs and data needed to perform job responsibilities and review access authority periodically to identify and correct inappropriate access;
- implement ID and password management controls across all computer platforms to maintain individual accountability and protect password confidentiality and test these controls periodically to ensure that they are operating effectively;
- develop targeted monitoring programs to routinely identify and investigate unusual or suspicious system and user access activity;
- restrict access to computer rooms based on job responsibility and periodically review this access to determine if it is still appropriate;
- separate incompatible computer responsibilities, such as system programming and security administration, and ensure that access controls enforce segregation of duties principles;
- require operating system software changes to be documented, authorized, tested, independently reviewed, and implemented by a third party; and
- establish controls to ensure that disaster recovery plans are comprehensive, current, fully tested, and maintained at the off-site storage facility.

We also recommend that you develop and implement a comprehensive departmentwide computer security planning and management program. Included in this program should be procedures for ensuring that

- security roles and responsibilities are clearly assigned and security management is given adequate attention;
- risks are assessed periodically to ensure that controls are appropriate;
- security policies and procedures comprehensively address all aspects of VA's interconnected environment;
- attempts (both successful and unsuccessful) to gain access to VA computer systems and the sensitive data files and critical production programs stored on these systems are identified, reported, and reviewed on a regular basis; and

- a security oversight function, including both ongoing local oversight and periodic external evaluations, is implemented to measure, test, and report on the effectiveness of controls.

In addition, we recommend that you direct the VA CIO to review and assess computer control weaknesses that have been identified throughout the department and establish a process to ensure that these weaknesses are addressed.

Furthermore, we recommend that you direct the VA CIO to monitor and periodically report on the status of actions taken to improve computer security throughout the department.

Finally, we recommend that you report the information system security weaknesses we identified as material internal control weaknesses in the department's FMFIA report until these weaknesses are corrected.

Agency Comments

In commenting on a draft of this report, VA agreed with our recommendations and stated that it is taking immediate action to correct computer control weaknesses and implement oversight mechanisms to ensure that these problems do not recur. VA stated that it is also preparing a comprehensive security plan and management program that will incorporate a risk management cycle and include requirements and guidance for monitoring access activity at VA facilities.

In addition, the VA stated that its CIO is working closely with the VBA and VHA CIOs to identify computer control weaknesses previously reported in OIG reviews and other internal evaluations and develop a plan to correct these deficiencies. VA also informed us that the CIO will report periodically to the OIG on VA's progress in correcting computer control weaknesses throughout the department.

Finally, VA agreed to consider outstanding computer control weaknesses for reporting as material weaknesses in the department's fiscal year 1998 FMFIA report when the department's top management council meets in the first quarter of fiscal year 1999.

This report contains recommendations to you. The head of a federal agency is required by 31 U.S.C. 720 to submit a written statement on actions taken on these recommendations to the Senate Committee on

Governmental Affairs and the House Committee on Government Reform and Oversight not later than 60 days after the date of this report. A written statement also must be sent to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of this report.

We are sending copies of the report to the Chairmen and Ranking Minority Members of the House and Senate Committees on Veterans Affairs and to the Director of the Office of Management and Budget. Copies will also be made available to others upon request.

Please contact me at (202) 512-3317 if you or your staff have any questions. Major contributors to this report are listed in appendix II.

Sincerely yours,

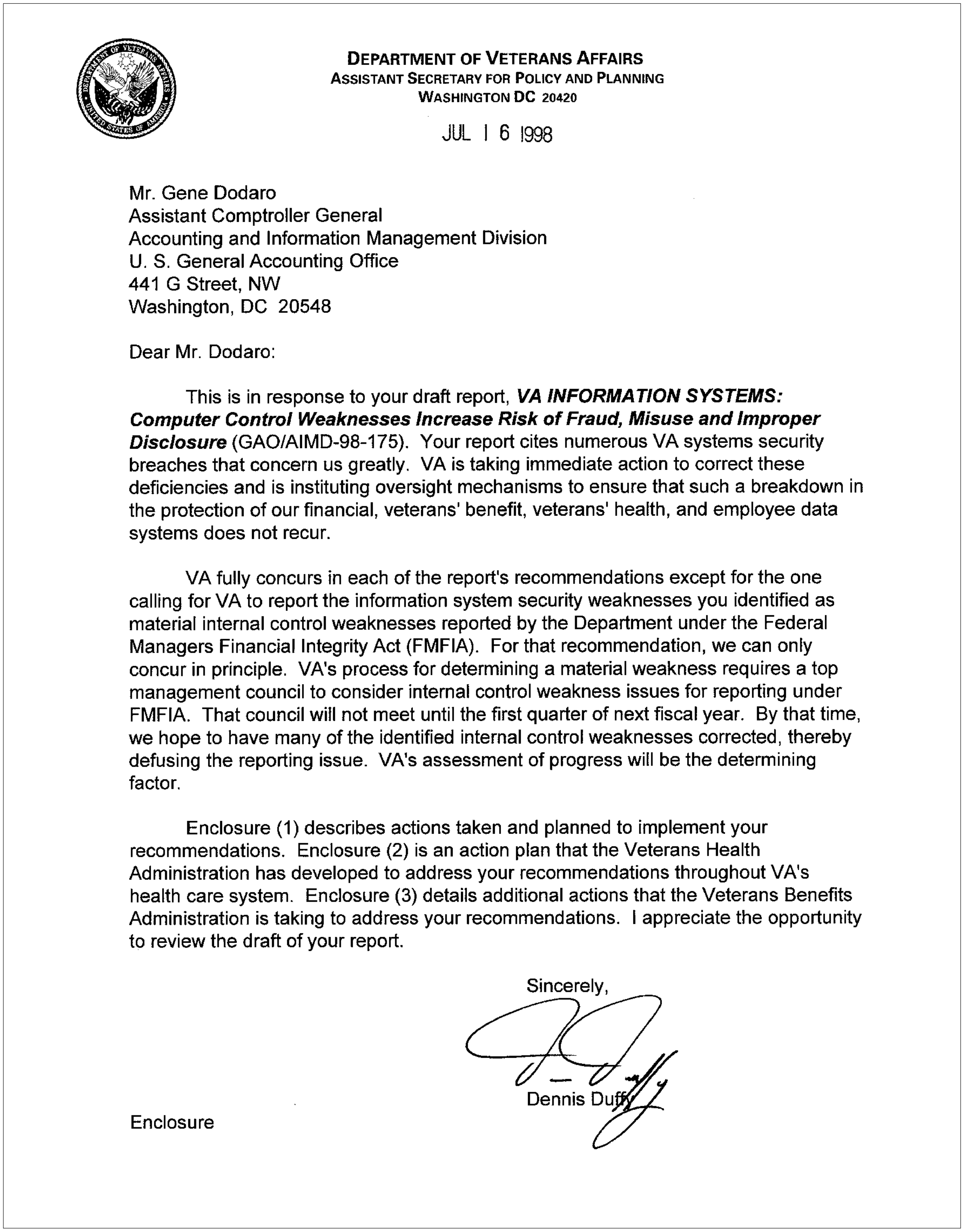
Robert F. Dacey

Robert F. Dacey
Director, Consolidated Audit and
Computer Security Issues

Appendix I

Comments From the Department of Veterans Affairs

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



DEPARTMENT OF VETERANS AFFAIRS
ASSISTANT SECRETARY FOR POLICY AND PLANNING
WASHINGTON DC 20420

JUL 1 6 1998

Mr. Gene Dodaro
Assistant Comptroller General
Accounting and Information Management Division
U. S. General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Dodaro:

This is in response to your draft report, ***VA INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure*** (GAO/AIMD-98-175). Your report cites numerous VA systems security breaches that concern us greatly. VA is taking immediate action to correct these deficiencies and is instituting oversight mechanisms to ensure that such a breakdown in the protection of our financial, veterans' benefit, veterans' health, and employee data systems does not recur.

VA fully concurs in each of the report's recommendations except for the one calling for VA to report the information system security weaknesses you identified as material internal control weaknesses reported by the Department under the Federal Managers Financial Integrity Act (FMFIA). For that recommendation, we can only concur in principle. VA's process for determining a material weakness requires a top management council to consider internal control weakness issues for reporting under FMFIA. That council will not meet until the first quarter of next fiscal year. By that time, we hope to have many of the identified internal control weaknesses corrected, thereby defusing the reporting issue. VA's assessment of progress will be the determining factor.

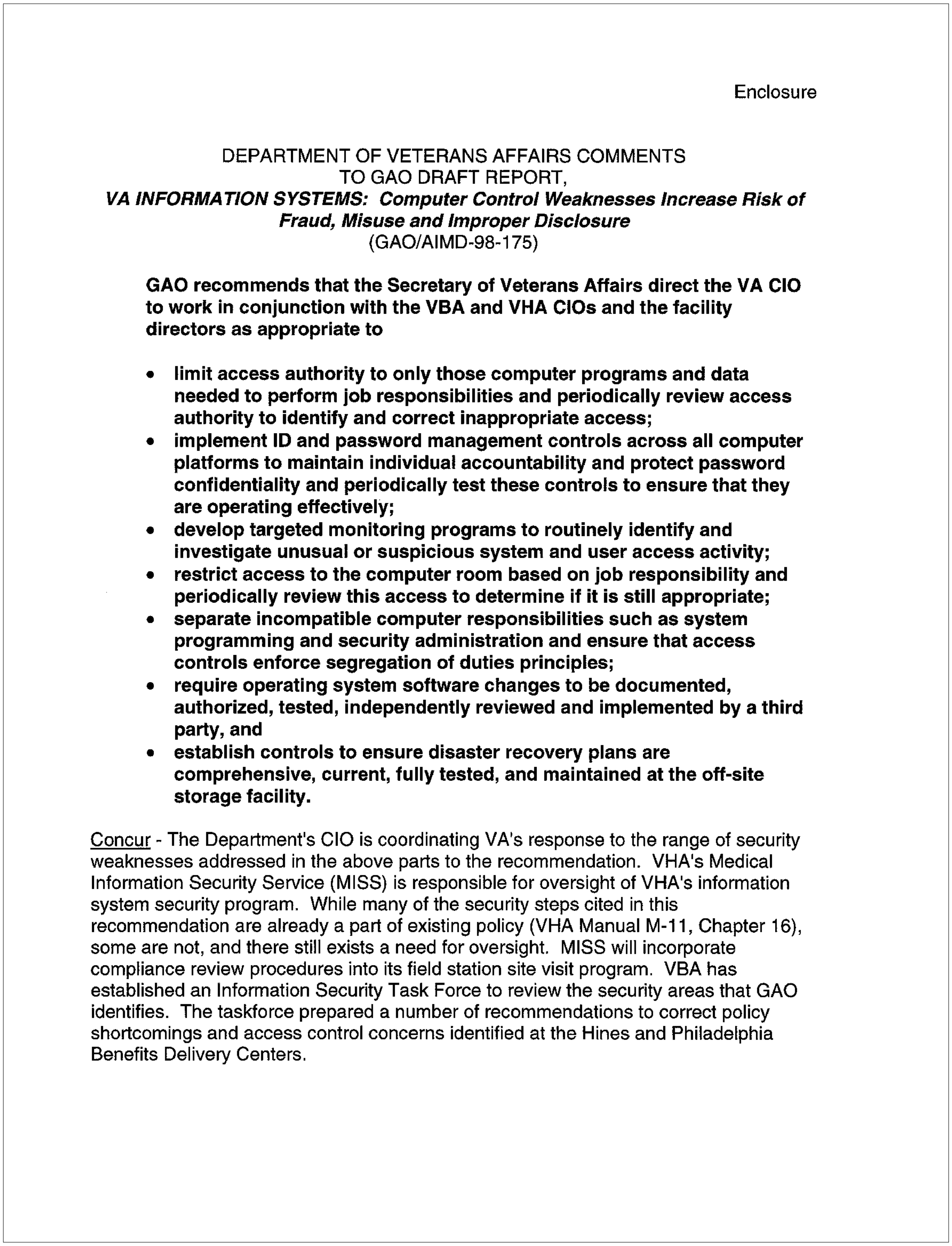
See comment 1.

Enclosure (1) describes actions taken and planned to implement your recommendations. Enclosure (2) is an action plan that the Veterans Health Administration has developed to address your recommendations throughout VA's health care system. Enclosure (3) details additional actions that the Veterans Benefits Administration is taking to address your recommendations. I appreciate the opportunity to review the draft of your report.

Sincerely,

Dennis Duffy

Enclosure



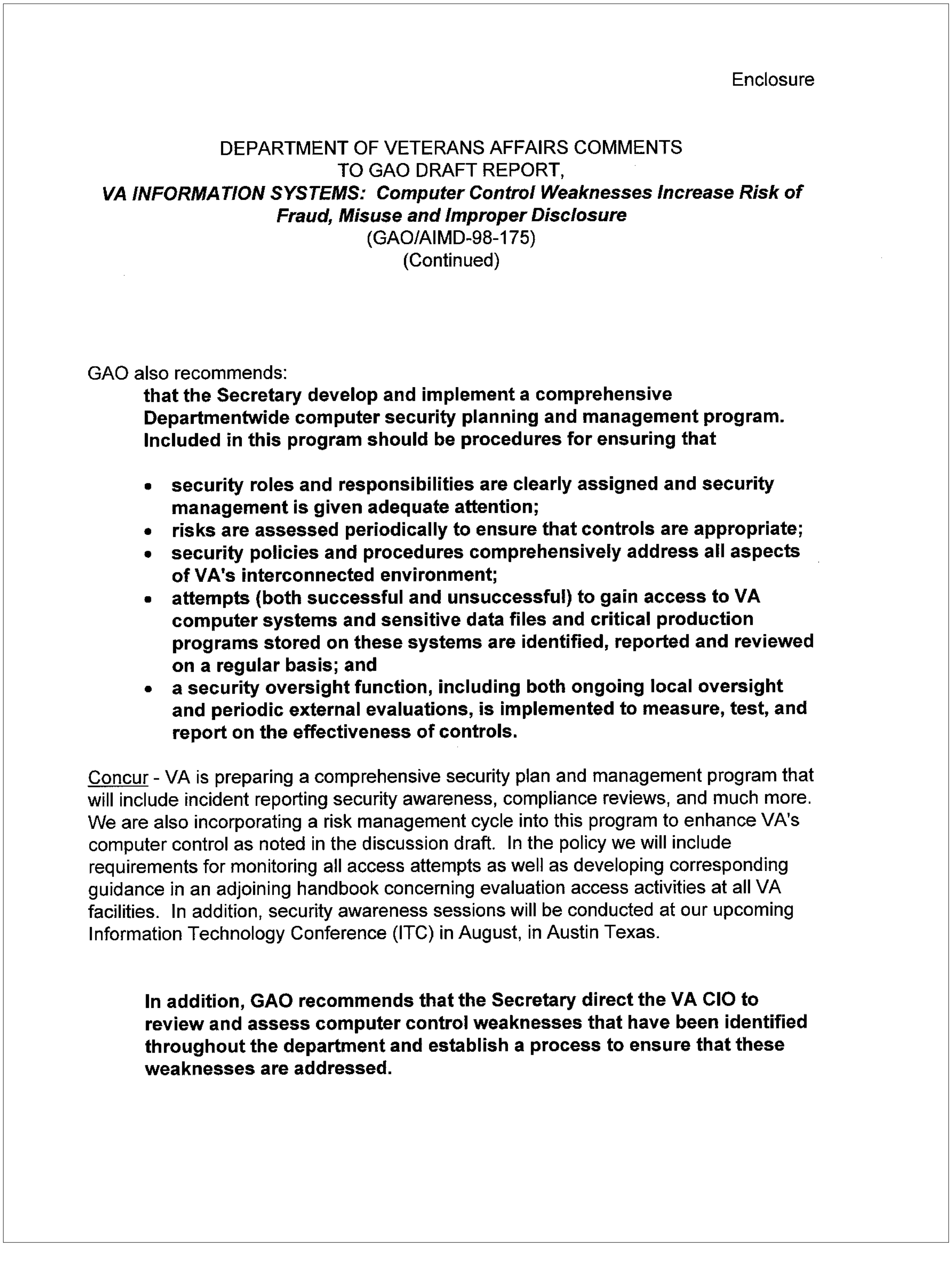
Enclosure

DEPARTMENT OF VETERANS AFFAIRS COMMENTS
TO GAO DRAFT REPORT,
VA INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure
(GAO/AIMD-98-175)

GAO recommends that the Secretary of Veterans Affairs direct the VA CIO to work in conjunction with the VBA and VHA CIOs and the facility directors as appropriate to

- **limit access authority to only those computer programs and data needed to perform job responsibilities and periodically review access authority to identify and correct inappropriate access;**
- **implement ID and password management controls across all computer platforms to maintain individual accountability and protect password confidentiality and periodically test these controls to ensure that they are operating effectively;**
- **develop targeted monitoring programs to routinely identify and investigate unusual or suspicious system and user access activity;**
- **restrict access to the computer room based on job responsibility and periodically review this access to determine if it is still appropriate;**
- **separate incompatible computer responsibilities such as system programming and security administration and ensure that access controls enforce segregation of duties principles;**
- **require operating system software changes to be documented, authorized, tested, independently reviewed and implemented by a third party, and**
- **establish controls to ensure disaster recovery plans are comprehensive, current, fully tested, and maintained at the off-site storage facility.**

Concur - The Department's CIO is coordinating VA's response to the range of security weaknesses addressed in the above parts to the recommendation. VHA's Medical Information Security Service (MISS) is responsible for oversight of VHA's information system security program. While many of the security steps cited in this recommendation are already a part of existing policy (VHA Manual M-11, Chapter 16), some are not, and there still exists a need for oversight. MISS will incorporate compliance review procedures into its field station site visit program. VBA has established an Information Security Task Force to review the security areas that GAO identifies. The taskforce prepared a number of recommendations to correct policy shortcomings and access control concerns identified at the Hines and Philadelphia Benefits Delivery Centers.



Enclosure

DEPARTMENT OF VETERANS AFFAIRS COMMENTS
TO GAO DRAFT REPORT,
VA INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure
(GAO/AIMD-98-175)
(Continued)

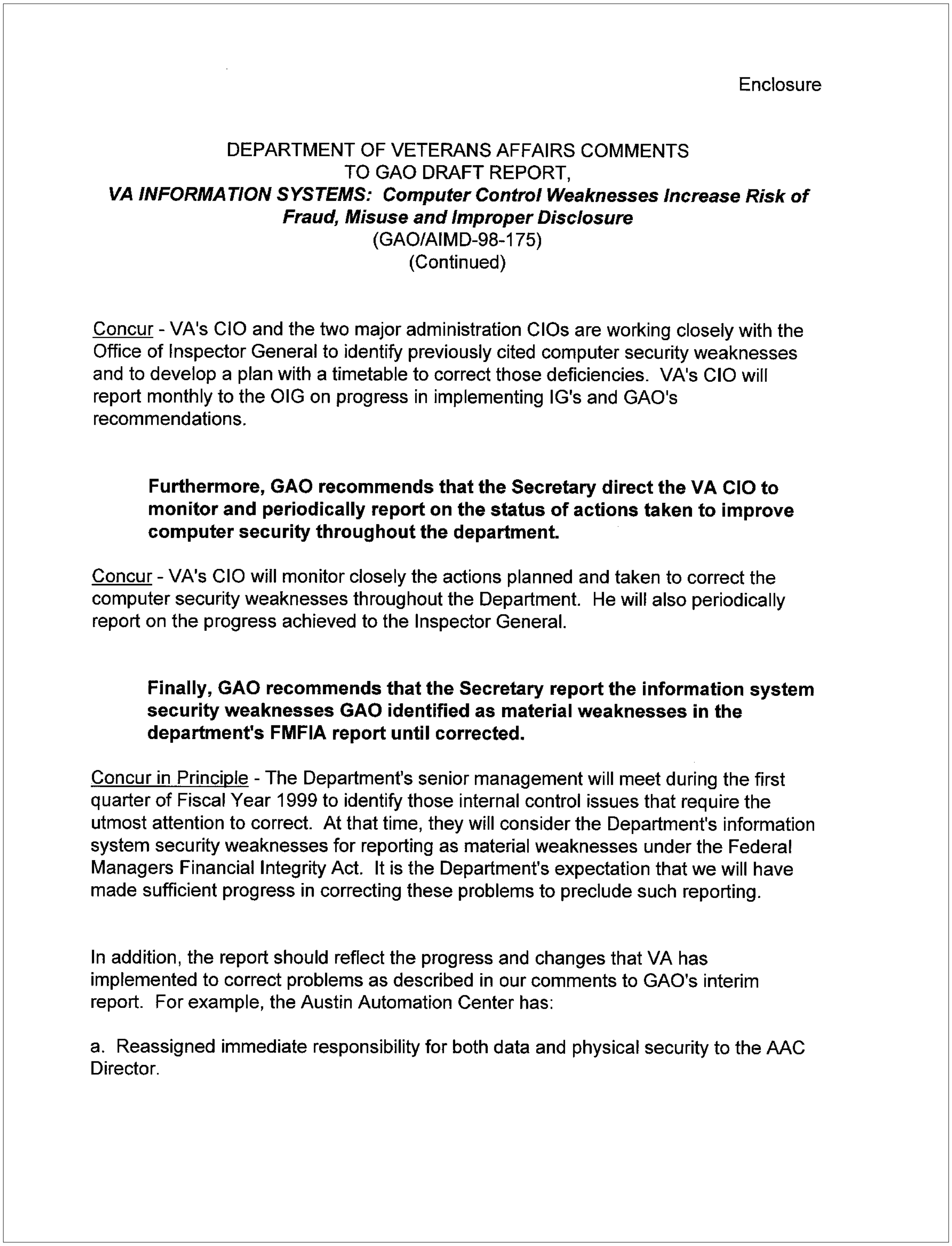
GAO also recommends:

that the Secretary develop and implement a comprehensive Departmentwide computer security planning and management program. Included in this program should be procedures for ensuring that

- **security roles and responsibilities are clearly assigned and security management is given adequate attention;**
- **risks are assessed periodically to ensure that controls are appropriate;**
- **security policies and procedures comprehensively address all aspects of VA's interconnected environment;**
- **attempts (both successful and unsuccessful) to gain access to VA computer systems and sensitive data files and critical production programs stored on these systems are identified, reported and reviewed on a regular basis; and**
- **a security oversight function, including both ongoing local oversight and periodic external evaluations, is implemented to measure, test, and report on the effectiveness of controls.**

Concur - VA is preparing a comprehensive security plan and management program that will include incident reporting security awareness, compliance reviews, and much more. We are also incorporating a risk management cycle into this program to enhance VA's computer control as noted in the discussion draft. In the policy we will include requirements for monitoring all access attempts as well as developing corresponding guidance in an adjoining handbook concerning evaluation access activities at all VA facilities. In addition, security awareness sessions will be conducted at our upcoming Information Technology Conference (ITC) in August, in Austin Texas.

In addition, GAO recommends that the Secretary direct the VA CIO to review and assess computer control weaknesses that have been identified throughout the department and establish a process to ensure that these weaknesses are addressed.



Enclosure

DEPARTMENT OF VETERANS AFFAIRS COMMENTS
TO GAO DRAFT REPORT,
VA INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure
(GAO/AIMD-98-175)
(Continued)

Concur - VA's CIO and the two major administration CIOs are working closely with the Office of Inspector General to identify previously cited computer security weaknesses and to develop a plan with a timetable to correct those deficiencies. VA's CIO will report monthly to the OIG on progress in implementing IG's and GAO's recommendations.

Furthermore, GAO recommends that the Secretary direct the VA CIO to monitor and periodically report on the status of actions taken to improve computer security throughout the department.

Concur - VA's CIO will monitor closely the actions planned and taken to correct the computer security weaknesses throughout the Department. He will also periodically report on the progress achieved to the Inspector General.

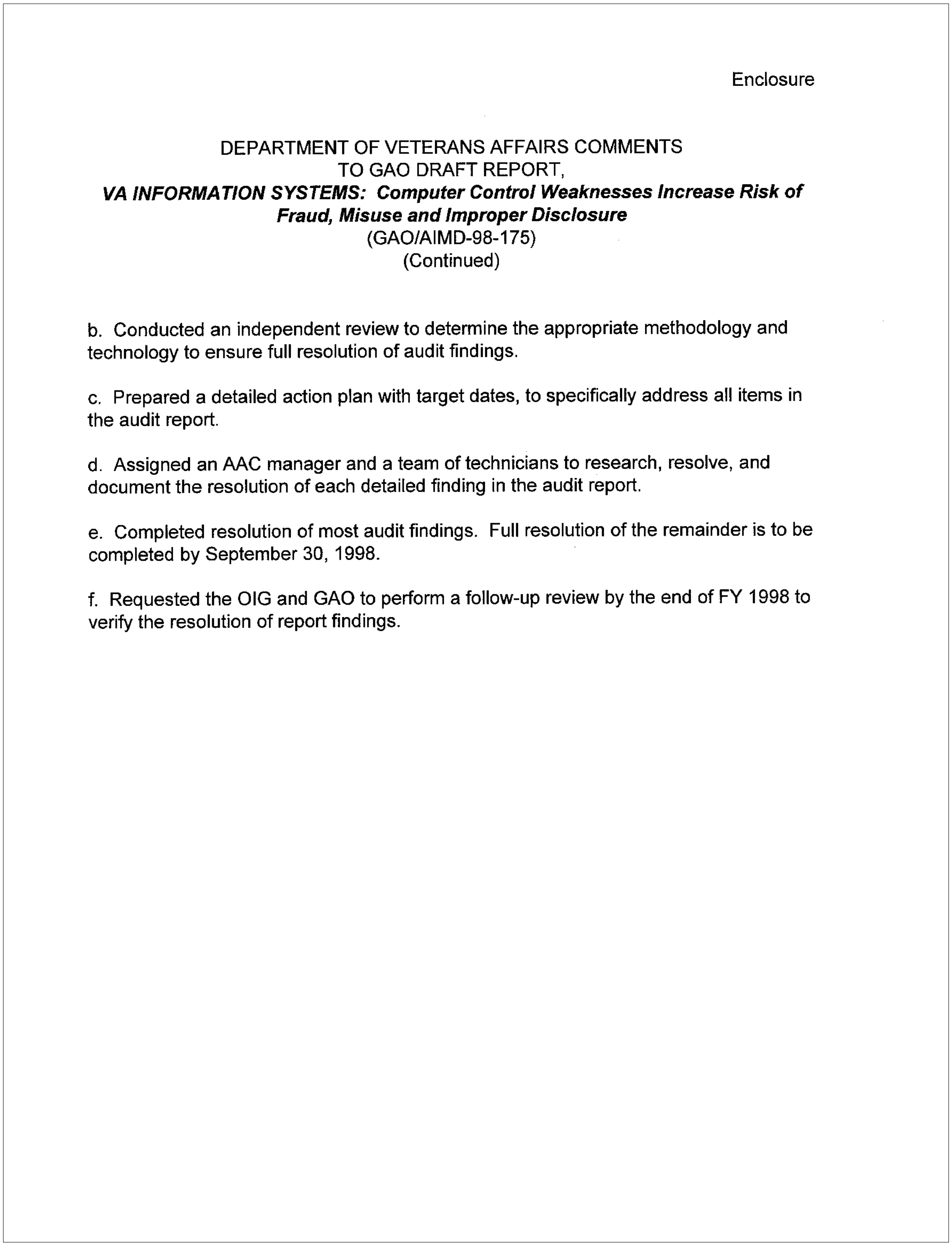
Finally, GAO recommends that the Secretary report the information system security weaknesses GAO identified as material weaknesses in the department's FMFIA report until corrected.

See comment 1.

Concur in Principle - The Department's senior management will meet during the first quarter of Fiscal Year 1999 to identify those internal control issues that require the utmost attention to correct. At that time, they will consider the Department's information system security weaknesses for reporting as material weaknesses under the Federal Managers Financial Integrity Act. It is the Department's expectation that we will have made sufficient progress in correcting these problems to preclude such reporting.

In addition, the report should reflect the progress and changes that VA has implemented to correct problems as described in our comments to GAO's interim report. For example, the Austin Automation Center has:

a. Reassigned immediate responsibility for both data and physical security to the AAC Director.



Enclosure

DEPARTMENT OF VETERANS AFFAIRS COMMENTS
TO GAO DRAFT REPORT,
VA INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure
(GAO/AIMD-98-175)
(Continued)

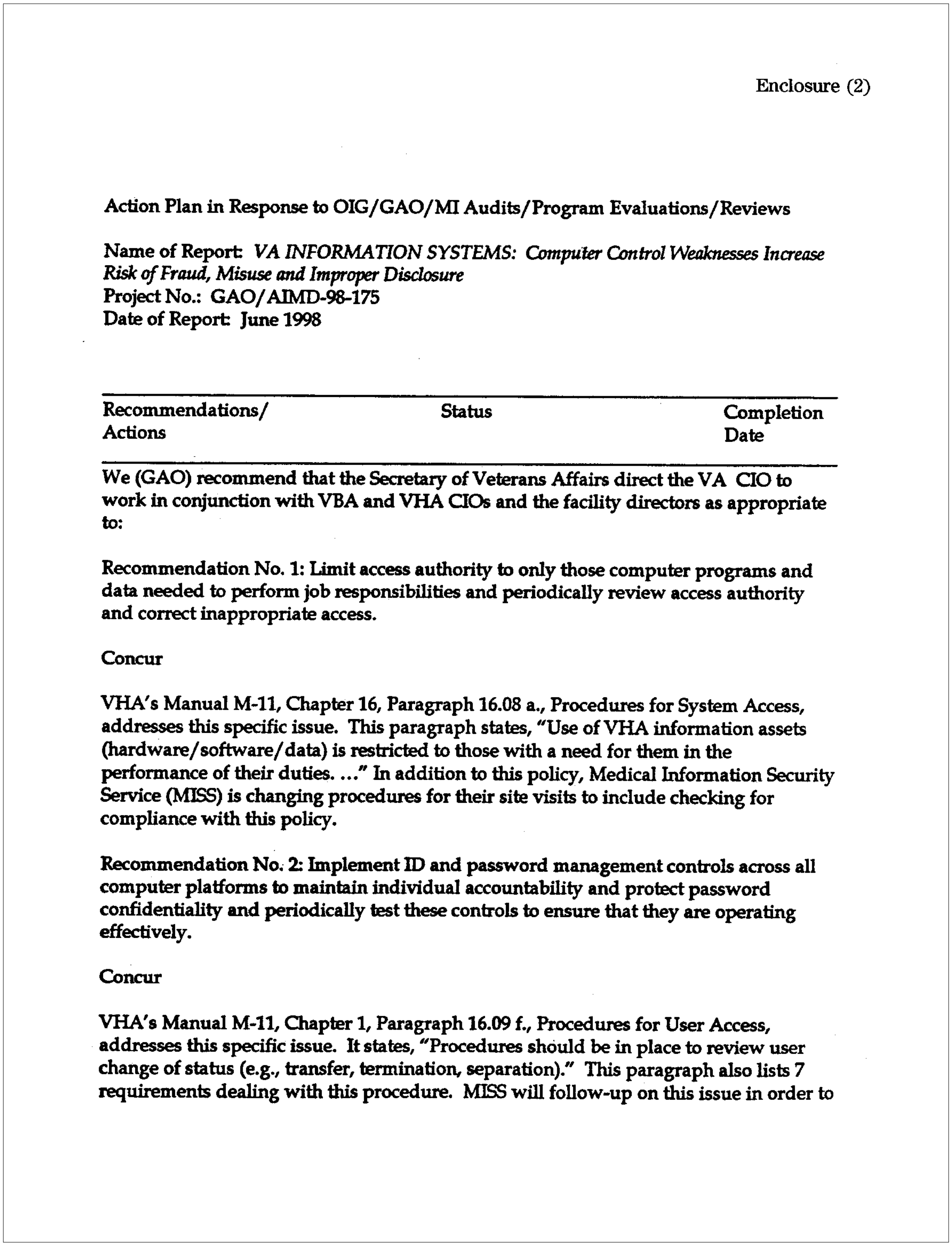
b. Conducted an independent review to determine the appropriate methodology and technology to ensure full resolution of audit findings.

c. Prepared a detailed action plan with target dates, to specifically address all items in the audit report.

d. Assigned an AAC manager and a team of technicians to research, resolve, and document the resolution of each detailed finding in the audit report.

e. Completed resolution of most audit findings. Full resolution of the remainder is to be completed by September 30, 1998.

f. Requested the OIG and GAO to perform a follow-up review by the end of FY 1998 to verify the resolution of report findings.



Enclosure (2)

Action Plan in Response to OIG/GAO/MI Audits/Program Evaluations/Reviews

Name of Report: *VA INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure*
Project No.: GAO/AIMD-98-175
Date of Report: June 1998

Recommendations/ Actions	Status	Completion Date

We (GAO) recommend that the Secretary of Veterans Affairs direct the VA CIO to work in conjunction with VBA and VHA CIOs and the facility directors as appropriate to:

Recommendation No. 1: Limit access authority to only those computer programs and data needed to perform job responsibilities and periodically review access authority and correct inappropriate access.

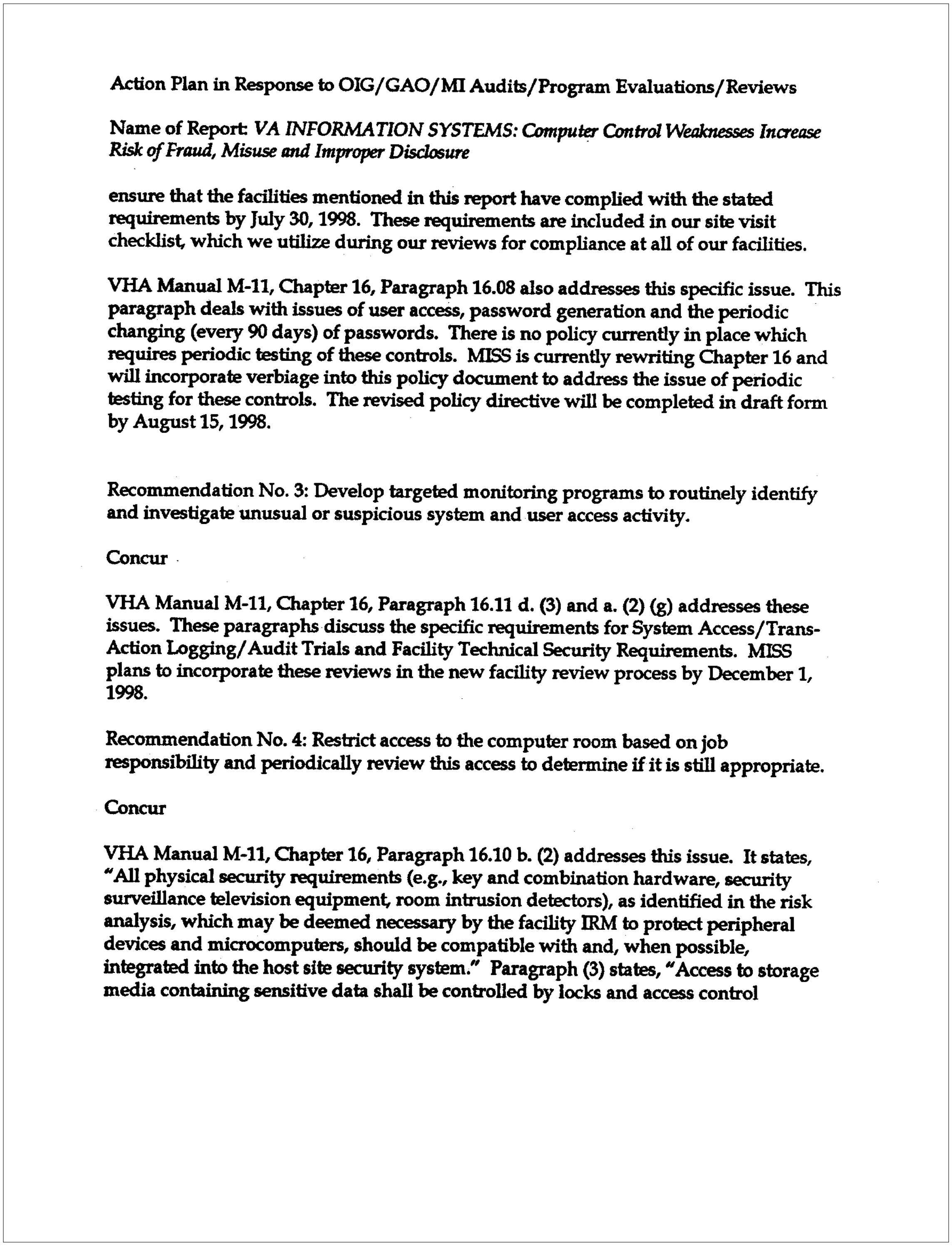
Concur

VHA's Manual M-11, Chapter 16, Paragraph 16.08 a., Procedures for System Access, addresses this specific issue. This paragraph states, "Use of VHA information assets (hardware/software/data) is restricted to those with a need for them in the performance of their duties. ..." In addition to this policy, Medical Information Security Service (MISS) is changing procedures for their site visits to include checking for compliance with this policy.

Recommendation No. 2: Implement ID and password management controls across all computer platforms to maintain individual accountability and protect password confidentiality and periodically test these controls to ensure that they are operating effectively.

Concur

VHA's Manual M-11, Chapter 1, Paragraph 16.09 f., Procedures for User Access, addresses this specific issue. It states, "Procedures should be in place to review user change of status (e.g., transfer, termination, separation)." This paragraph also lists 7 requirements dealing with this procedure. MISS will follow-up on this issue in order to



Action Plan in Response to OIG/GAO/MI Audits/Program Evaluations/Reviews

Name of Report: *VA INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure*

ensure that the facilities mentioned in this report have complied with the stated requirements by July 30, 1998. These requirements are included in our site visit checklist, which we utilize during our reviews for compliance at all of our facilities.

VHA Manual M-11, Chapter 16, Paragraph 16.08 also addresses this specific issue. This paragraph deals with issues of user access, password generation and the periodic changing (every 90 days) of passwords. There is no policy currently in place which requires periodic testing of these controls. MISS is currently rewriting Chapter 16 and will incorporate verbiage into this policy document to address the issue of periodic testing for these controls. The revised policy directive will be completed in draft form by August 15, 1998.

Recommendation No. 3: Develop targeted monitoring programs to routinely identify and investigate unusual or suspicious system and user access activity.

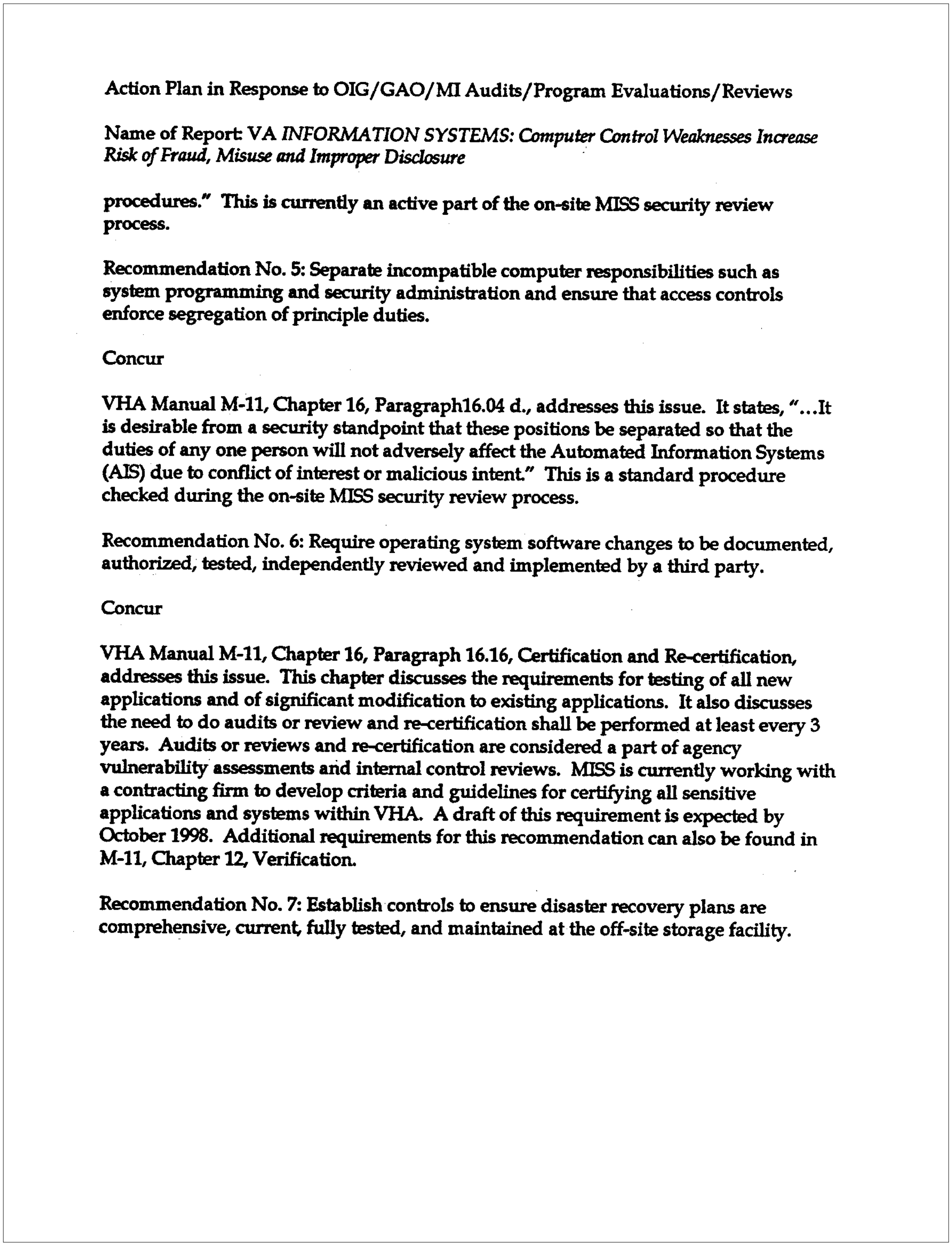
Concur

VHA Manual M-11, Chapter 16, Paragraph 16.11 d. (3) and a. (2) (g) addresses these issues. These paragraphs discuss the specific requirements for System Access/Trans-Action Logging/Audit Trials and Facility Technical Security Requirements. MISS plans to incorporate these reviews in the new facility review process by December 1, 1998.

Recommendation No. 4: Restrict access to the computer room based on job responsibility and periodically review this access to determine if it is still appropriate.

Concur

VHA Manual M-11, Chapter 16, Paragraph 16.10 b. (2) addresses this issue. It states, "All physical security requirements (e.g., key and combination hardware, security surveillance television equipment, room intrusion detectors), as identified in the risk analysis, which may be deemed necessary by the facility IRM to protect peripheral devices and microcomputers, should be compatible with and, when possible, integrated into the host site security system." Paragraph (3) states, "Access to storage media containing sensitive data shall be controlled by locks and access control



Action Plan in Response to OIG/GAO/MI Audits/Program Evaluations/Reviews

Name of Report: VA *INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure*

procedures." This is currently an active part of the on-site MISS security review process.

Recommendation No. 5: Separate incompatible computer responsibilities such as system programming and security administration and ensure that access controls enforce segregation of principle duties.

Concur

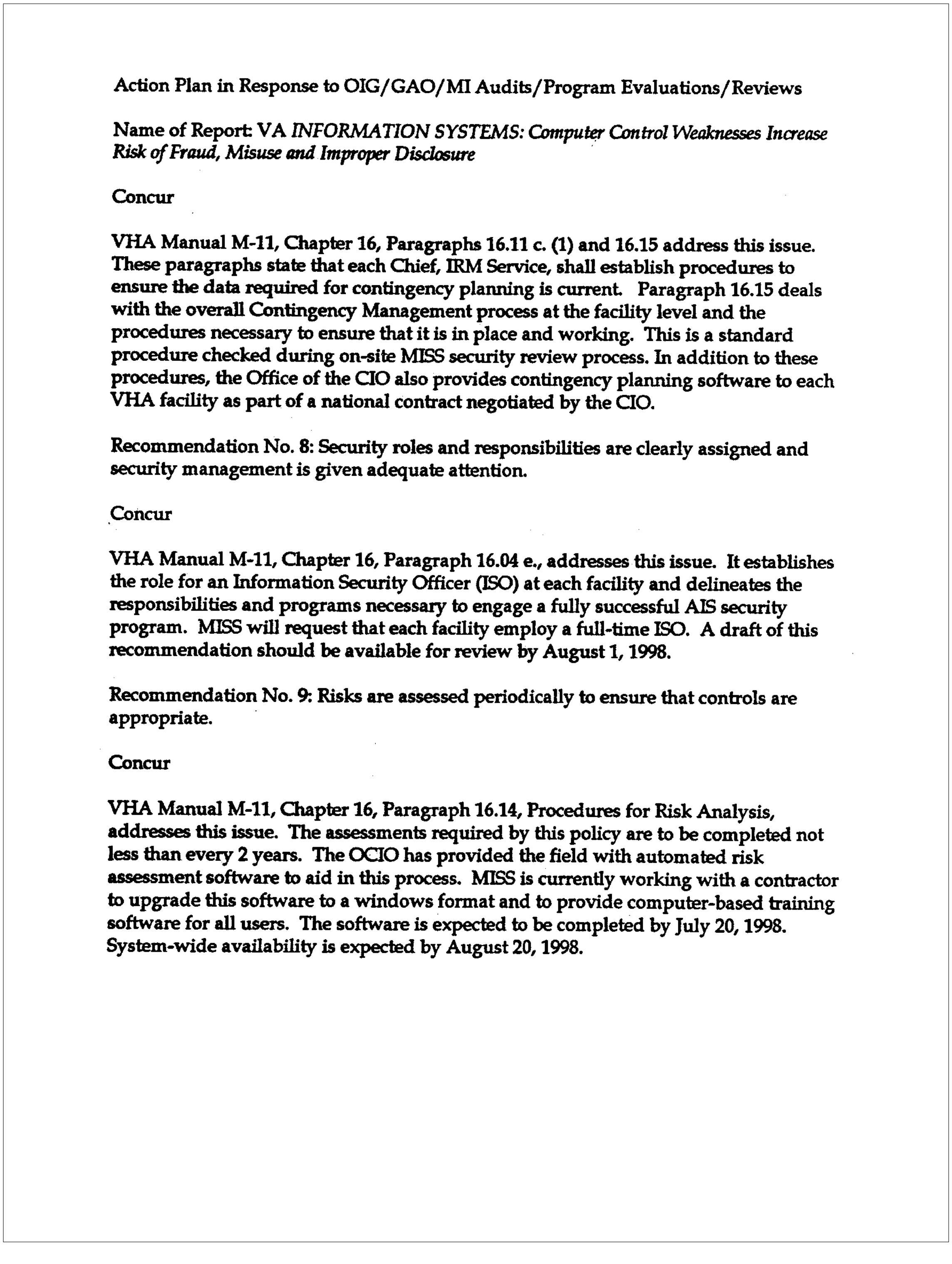
VHA Manual M-11, Chapter 16, Paragraph16.04 d., addresses this issue. It states, "...It is desirable from a security standpoint that these positions be separated so that the duties of any one person will not adversely affect the Automated Information Systems (AIS) due to conflict of interest or malicious intent." This is a standard procedure checked during the on-site MISS security review process.

Recommendation No. 6: Require operating system software changes to be documented, authorized, tested, independently reviewed and implemented by a third party.

Concur

VHA Manual M-11, Chapter 16, Paragraph 16.16, Certification and Re-certification, addresses this issue. This chapter discusses the requirements for testing of all new applications and of significant modification to existing applications. It also discusses the need to do audits or review and re-certification shall be performed at least every 3 years. Audits or reviews and re-certification are considered a part of agency vulnerability assessments and internal control reviews. MISS is currently working with a contracting firm to develop criteria and guidelines for certifying all sensitive applications and systems within VHA. A draft of this requirement is expected by October 1998. Additional requirements for this recommendation can also be found in M-11, Chapter 12, Verification.

Recommendation No. 7: Establish controls to ensure disaster recovery plans are comprehensive, current, fully tested, and maintained at the off-site storage facility.



Action Plan in Response to OIG/GAO/MI Audits/Program Evaluations/Reviews

Name of Report: VA *INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure*

Concur

VHA Manual M-11, Chapter 16, Paragraphs 16.11 c. (1) and 16.15 address this issue. These paragraphs state that each Chief, IRM Service, shall establish procedures to ensure the data required for contingency planning is current. Paragraph 16.15 deals with the overall Contingency Management process at the facility level and the procedures necessary to ensure that it is in place and working. This is a standard procedure checked during on-site MISS security review process. In addition to these procedures, the Office of the CIO also provides contingency planning software to each VHA facility as part of a national contract negotiated by the CIO.

Recommendation No. 8: Security roles and responsibilities are clearly assigned and security management is given adequate attention.

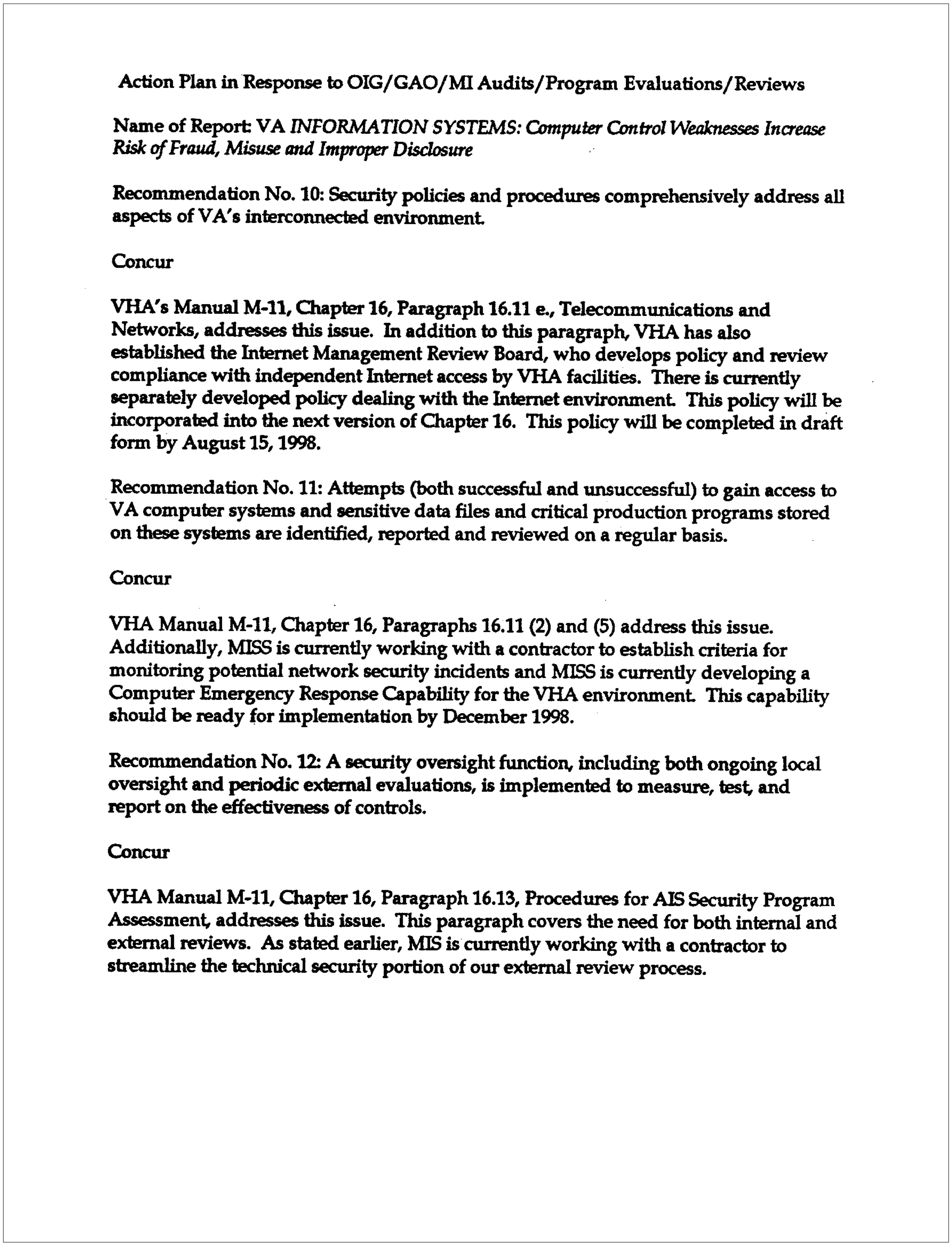
Concur

VHA Manual M-11, Chapter 16, Paragraph 16.04 e., addresses this issue. It establishes the role for an Information Security Officer (ISO) at each facility and delineates the responsibilities and programs necessary to engage a fully successful AIS security program. MISS will request that each facility employ a full-time ISO. A draft of this recommendation should be available for review by August 1, 1998.

Recommendation No. 9: Risks are assessed periodically to ensure that controls are appropriate.

Concur

VHA Manual M-11, Chapter 16, Paragraph 16.14, Procedures for Risk Analysis, addresses this issue. The assessments required by this policy are to be completed not less than every 2 years. The OCIO has provided the field with automated risk assessment software to aid in this process. MISS is currently working with a contractor to upgrade this software to a windows format and to provide computer-based training software for all users. The software is expected to be completed by July 20, 1998. System-wide availability is expected by August 20, 1998.



Action Plan in Response to OIG/GAO/MI Audits/Program Evaluations/Reviews

Name of Report: VA *INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure*

Recommendation No. 10: Security policies and procedures comprehensively address all aspects of VA's interconnected environment.

Concur

VHA's Manual M-11, Chapter 16, Paragraph 16.11 e., Telecommunications and Networks, addresses this issue. In addition to this paragraph, VHA has also established the Internet Management Review Board, who develops policy and review compliance with independent Internet access by VHA facilities. There is currently separately developed policy dealing with the Internet environment. This policy will be incorporated into the next version of Chapter 16. This policy will be completed in draft form by August 15, 1998.

Recommendation No. 11: Attempts (both successful and unsuccessful) to gain access to VA computer systems and sensitive data files and critical production programs stored on these systems are identified, reported and reviewed on a regular basis.

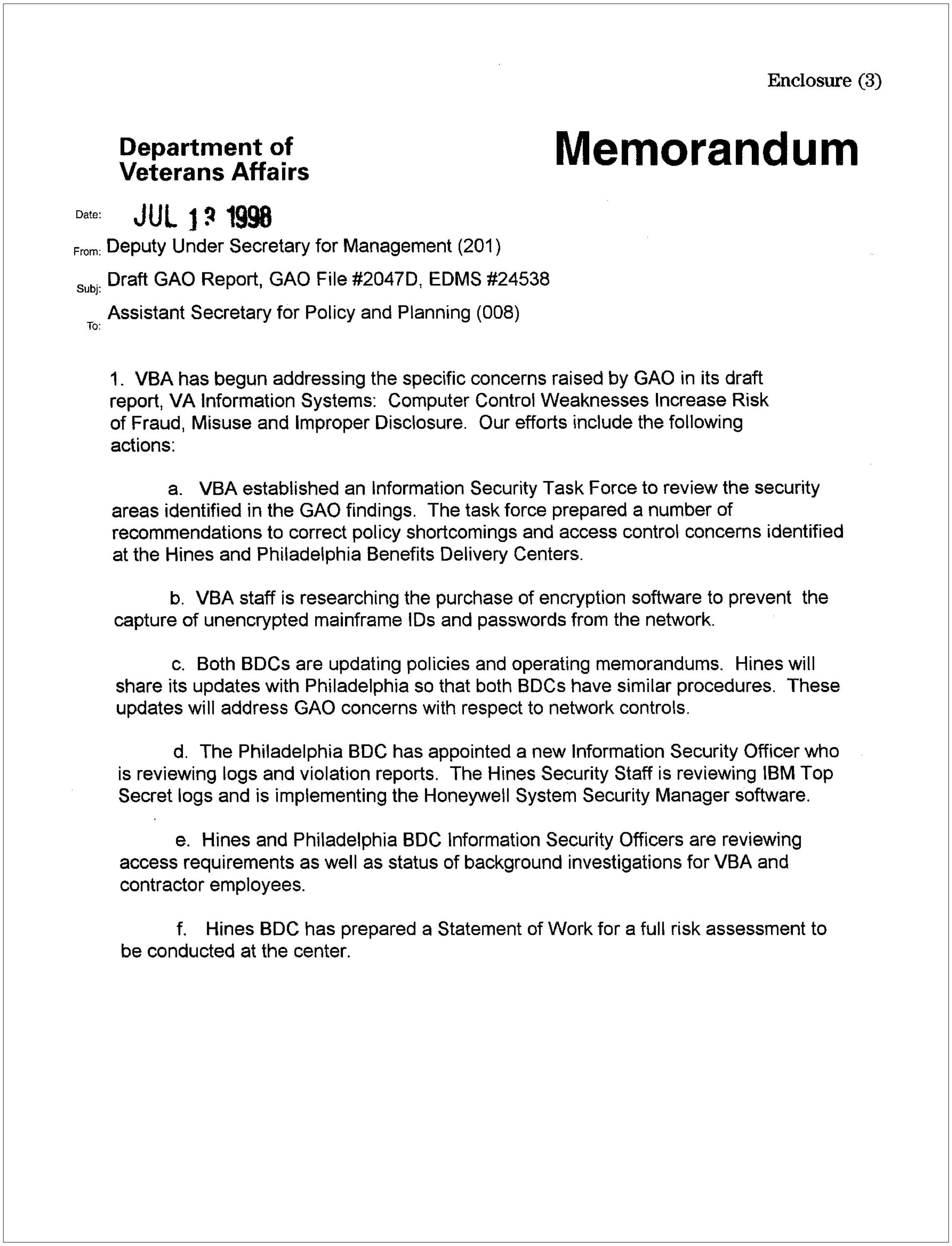
Concur

VHA Manual M-11, Chapter 16, Paragraphs 16.11 (2) and (5) address this issue. Additionally, MISS is currently working with a contractor to establish criteria for monitoring potential network security incidents and MISS is currently developing a Computer Emergency Response Capability for the VHA environment. This capability should be ready for implementation by December 1998.

Recommendation No. 12: A security oversight function, including both ongoing local oversight and periodic external evaluations, is implemented to measure, test, and report on the effectiveness of controls.

Concur

VHA Manual M-11, Chapter 16, Paragraph 16.13, Procedures for AIS Security Program Assessment, addresses this issue. This paragraph covers the need for both internal and external reviews. As stated earlier, MIS is currently working with a contractor to streamline the technical security portion of our external review process.



Enclosure (3)

**Department of
Veterans Affairs**

Memorandum

Date: JUL 13 1998

From: Deputy Under Secretary for Management (201)

Subj: Draft GAO Report, GAO File #2047D, EDMS #24538

To: Assistant Secretary for Policy and Planning (008)

1. VBA has begun addressing the specific concerns raised by GAO in its draft report, VA Information Systems: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure. Our efforts include the following actions:

a. VBA established an Information Security Task Force to review the security areas identified in the GAO findings. The task force prepared a number of recommendations to correct policy shortcomings and access control concerns identified at the Hines and Philadelphia Benefits Delivery Centers.

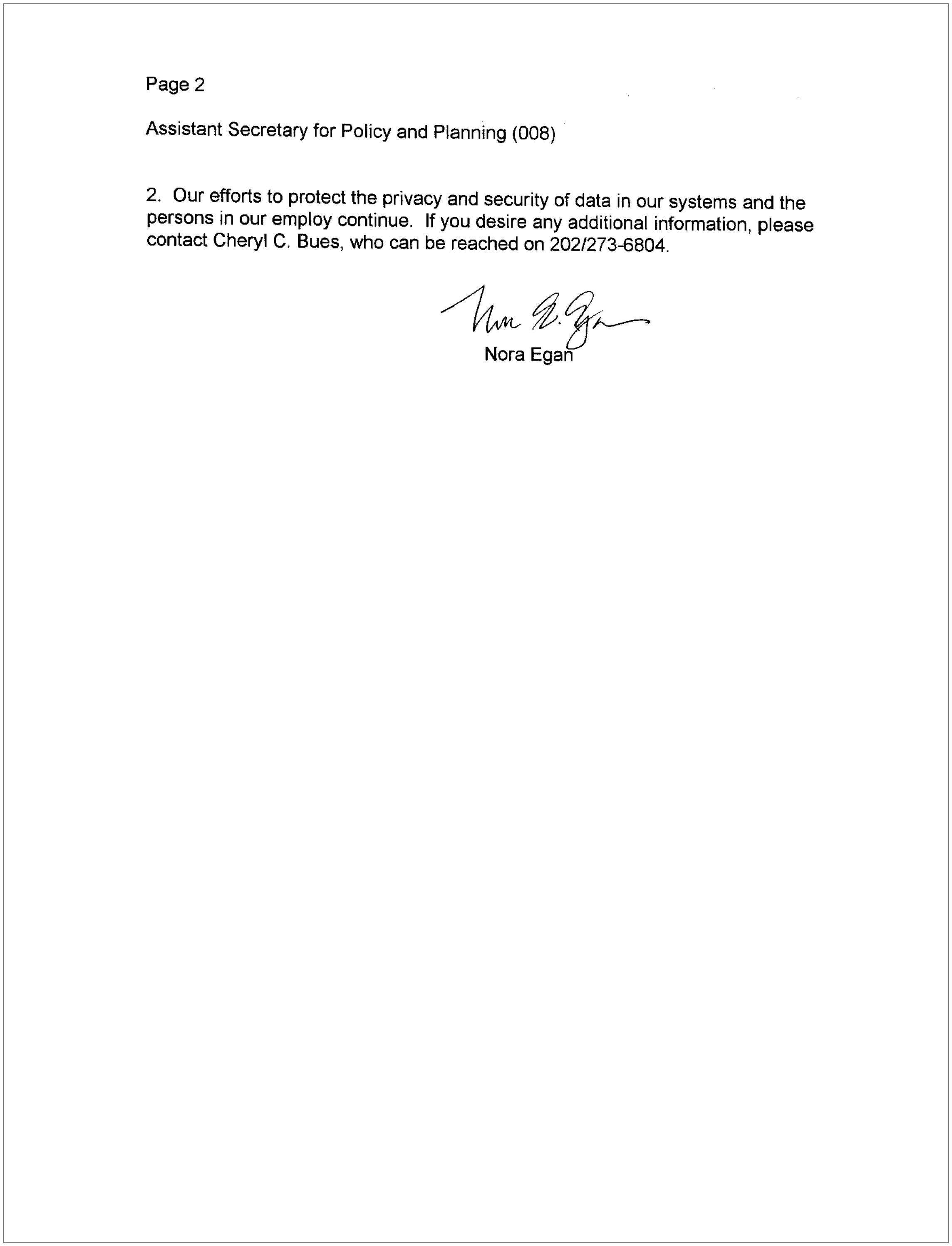
b. VBA staff is researching the purchase of encryption software to prevent the capture of unencrypted mainframe IDs and passwords from the network.

c. Both BDCs are updating policies and operating memorandums. Hines will share its updates with Philadelphia so that both BDCs have similar procedures. These updates will address GAO concerns with respect to network controls.

d. The Philadelphia BDC has appointed a new Information Security Officer who is reviewing logs and violation reports. The Hines Security Staff is reviewing IBM Top Secret logs and is implementing the Honeywell System Security Manager software.

e. Hines and Philadelphia BDC Information Security Officers are reviewing access requirements as well as status of background investigations for VBA and contractor employees.

f. Hines BDC has prepared a Statement of Work for a full risk assessment to be conducted at the center.



Page 2

Assistant Secretary for Policy and Planning (008)

2. Our efforts to protect the privacy and security of data in our systems and the persons in our employ continue. If you desire any additional information, please contact Cheryl C. Bues, who can be reached on 202/273-6804.

Nora Egan

The following is GAO's comment on the Department of Veterans Affairs' letter dated July 16, 1998.

GAO Comment

1. Although VA only concurred in principle with our recommendation to report the information system security weaknesses we identified as material internal control weaknesses in the department's FMFIA report, the department's plans for evaluating computer control weaknesses for reporting as material weaknesses appear reasonable. VA has committed to presenting outstanding control weaknesses to the top management council when it meets in the first quarter of fiscal year 1999 to determine material FMFIA weaknesses for fiscal year 1998.

Appendix I

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.

Lon C. Chin, Assistant Director
Edward M. Glagola, Jr., Assistant Director
Shane D. Hartzler, Senior Evaluator
Walter P. Opaska, Senior Evaluator
Christopher J. Warweg, Senior Evaluator

Atlanta Field Office

Sharon S. Kittrell, Senior Auditor

Dallas Field Office

David W. Irvin, Assistant Director
Debra M. Conner, Senior Auditor
Shannon Q. Cross, Senior Evaluator
Charles M. Vrabel, Senior Auditor

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO’s World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001